# 2021年CCF-绿盟科技“鲲鹏”科研基金重点资助课题

# 1.智能威胁分析与数据安全方向

### 面向安全运营的智能风险评估与事件关系推理

从大规模、多源、异构、多模态日志数据中有效识别复杂攻击模式与攻击意图，面临诸多关键科学挑战：1）关联缺失。跨网络与终端数据难以有效同步日志触发条件，导致多源日志之间难以有效关联建模；2）分析语义缺失，统计层次的规律难以反映攻击者底层的攻击意图与技战术方法；3）告警风险难以有效度量，告警误报引发告警应对疲劳；4）结构化、半结构、非结构化告警元信息及载荷数据难以提供统一的视角辅助告警分诊。面对以上挑战，为了有效识别特征、时序、图、时序图等多模态事件，研究通过多源多模态事件图谱构建，实现可解释的异常检测与威胁定位，挖掘事件元信息及上下文，进而进行关系推理，实现攻击路径溯源与取证，具有重要的研究价值。

**研究方向包括但不限于：**

1. 研究大规模、多模态事件日志的统一表示学习与建模方法，以及异常检测与风险评估算法，支撑根据关键线索、知识进行事件关系的抽取、消歧、关系生成，支持10种以上关键实体及事件关系抽取与关联，及相关图谱的构建及分析，TOP100异常事件误报率不高于10%；
2. 研究大规模告警载荷的增量表示学习，载荷关键词信息自动化标注，基于可解释人工智能的告警载荷关键依据提取，能够持5种以上类型告警的表示建模，自动标注准确率不低于80%；
3. 研究安全知识的表示方式以及与数据（网络侧告警日志与终端日志）的有效关联方式，以辅助攻击路径调查溯源，跨多源数据事件关联命中准确率不低于90%。

**研究输出成果：**

1. 相关原型系统（包括多模事件表示学习模型及异常检测、告警关键信息自动标注及事件关联溯源子系统），并提供源代码；
2. 相关研究报告、高水平学术论文、发明专利等。

### 数据智能化分类分级关键技术研究

在“以数据为中心”的数据安全领域，数据分类分级具有举足轻重的地位，其对于企业数据安全建设具有重要的价值与意义。实际上，它可以拆分为两个子任务——数据分类、数据分级，其中前者依据数据的来源、内容和用途对数据类别进行划分和归类；而后者根据数据价值、内容敏感程度、影响和分发范围不同对数据进行敏感级别划分。做好数据分类分级，一方面可满足企业自身数据安全运营的要求，将数据资产化，为企业提供精确的数据服务，以及不同粒度的数据安全防护与管理；另一方面可满足合规需求，一个重要里程碑是我国2021年通过的《数据安全法》中明确地将数据分类分级保护作为一项基本的制度。

针对数据分类分级场景中的数据分类，目前传统方法主要集中在基于正则表达式和基于关键词库的两类基本的识别方法；而对于数据分级，传统主要采用基于规则、策略的定级方法。然而这些传统方法面临着人力投入大、正则库和关键库的维护成本高、漏检率高、不够智能化（无法理解与识别类似的敏感信息）且也不易于扩展，极大地增加企业的运营成本。因此，引入人工智能（Artificial Intelligence，AI）技术成为业界普遍的共识。然而，简单地迁移AI方法也将面临着众多的问题与挑战：1) 数据类别分布的不平衡；2) 单个企业某些类别的样本量较少；3）数据分类涉及类别非常多，同时涉及增加新类别的题；4）每个企业独立训练模型造成资源浪费，复用性差；5）跨企业的联合AI建模涉及隐私、敏感数据问题。

**研究方向包括但不限于：**

1. 针对单个企业的AI建模场景，研究基于多分类（10类以上）、多标签学习任务的智能数据分类分级算法，如NLP、神经网络、随机森林等，在非平衡数据集上可取得较好的性能效果；
2. 针对多个企业无法联网的AI建模场景，研究基于增量学习的智能数据分类分级算法与框架，A企业的模型a可放在B企业进行微调学习得到模型b，同时研究可抵抗反演攻击的模型安全机制；
3. 针对多个企业可以联网的AI建模场景，研究基于联邦学习的智能数据分类分级算法与框架，交互通信轮数少，安全性高且可抵抗常见的隐私窃取攻击；
4. 结合区块链技术，研究安全、可信任、可追溯的跨企业联合AI建模的数据分类分级框架与系统。

**研究输出成果：**

1. 相关原型系统（包括基于增量学习、联邦学习的两类智能数据分类分级系统），并提供源代码；
2. 相关研究报告、高水平学术论文、发明专利等。

### 虚假信息的识别关键技术研究

由互联网传播，危害国家安全、网络空间安全的虚假信息，对线上和线下的群体行为起着重要的推动作用。它具有信源模糊性、受众敏感性、传播病毒性等特征，其在生成和传播过程中呈现着有别于一般网络舆情的特征。不仅仅严重影响着互联网信息生态系统的可信度，而且网络上的演化也在向现实生活中转移，这影响着网络空间安全、社会稳定。

**研究方向包括但不限于：**

1. 针对社交媒体场景，研究如何高效、精准的识别虚假信息的方法，能识别虚假信息种类不少于10种（如虚假购物消费、虚假贷款诈骗）；
2. 针对如短视频、直播等新型社交媒体平台出现的使用视频方式的虚假信息，研究如何有效筛查、识别虚假信息的方法，能针对至少2个主流短视频平台在线视频筛选虚假信息，误报率不高于20%；
3. 针对网络威胁情报收集场景，研究情报信息内容真实性识别技术，能完成大规模收集威胁情报场景下，甄别冲突情况下情报信息（STIX 2.0规范）判断方法和意图推测。

**研究输出成果：**

1. 相关原型系统（包括针对具体场景的虚假数据智能识别算法，及训练、验证数据集），并提供源代码；
2. 相关研究报告、高水平学术论文、发明专利等。

### 面向社交网络黑客社区发现及其相关应用的技术研究

在计算机网络安全事件中，网络安全研究相关人员和群组是非常重要的关注对象，其中就包括专门从事破坏网络安全的“黑客”和他们所在的黑客组织。了解和掌握这些黑客及其组织的行为有助于增强对网络安全态势的感知能力，提前预测网络安全事件的发生或者在发生网络攻击后尽快确定攻击发起人。要实现对黑客及其组织的监视和了解，社交网络网站和黑客论坛成为最重要的信息来源。利用社交网络分析可以明确黑客团体的生态系统结构，进一步应用可区分团体内的关键人物（节点）、对隐藏的潜在重要成员（离群点）进行识别以及对跨平台用户进行识别等。因此，通过社交网络分析来探究黑客团体及其活动有很大的研究价值。

**研究方向包括但不限于：**

1. 研究数据收集与预处理机制。针对研究对象（某一地区或者某一国家黑客群体），在少量种子用户（节点）的基础上采用雪球采样法爬取Twitter或者黑客论坛等社交网络上的数据。爬取的数据包括用户ID、用户地址坐标、用户关注者和被关注者、用户发布的内容、用户之间的交互活动等。收集的数据，尤其是用户发布的内容需要经过大小写处理、去除停用词和非法字符、词干提取等预处理流程，以方便后续进行文本相似性分析；
2. 研究可划分社交网络子社区的社区发现算法；
3. 研究社区发现扩展应用，在社交网络社区发现的基础上，可进一步执行子社区内关键节点的识别和预测社区外节点与社区产生链接的可能，包括未知的链接以及未来可能的链接。

**研究输出成果：**

1. 相关原型系统，并提供源代码；
2. 相关研究报告、高水平学术论文、发明专利等。

### 基于零样本或小样本学习的深度异常检测技术研究

为了实现对未知攻击行为的检测，在当前的安全分析过程中会采集大量体现用户行为的数据，如主机日志、应用日志、网络流量元数据、安全设备告警等。这些数据往往是正常行为数据和攻击行为数据混杂在一起，没有进行标注，或只有少量数据得到了标注。如何在无异常样本的训练集的情况下，从海量的正常行为数据中准确识别随机性攻击行为，是一项具有很高的学术价值和实际应用价值的研究课题。

**研究方向包括但不限于：**

1. 研究面向没有异常样本训练集的异常行为检测的关键技术，提供至少1种零样本或小样本深度异常检测算法，能够找出数据中的异常点、上下文异常、集体或群体异常；
2. 研究一种零样本学习方法， 从没有异常样本的训练集中识别异常行为；
3. 研究小样本学习方法，针对少量标注后的数据，实现异常行为检测。

**研究输出成果：**

1. 相关原型系统及算法，并提供源代码；
2. 相关研究报告、高水平学术论文、发明专利等。

### 面向区块链去中心化金融系统的异常行为检测和防护技术研究

基于区块链的去中心化应用生态发展迅速，具有高价值、高回报、高波动性的特点。然而随着去中心化金融系统承载资产价值的快速增加，相应攻击行为也变得日益频繁，且往往能造成较大破坏。由于区块链具有匿名化、账本不可篡改等特点，针对区块链的异常行为检测和防护与传统技术具有显著区别，同时也符合当下工业界迫切的应用需求。

**研究方向包括但不限于：**

1. 研究面向区块链去中心化金融系统的异常交易行为检测技术，基于账本、区块链日志、交易池数据的实时分析，快速识别异常交易行为或恶意攻击，分析待提交交易的潜在钓鱼、抢跑风险，进而实现对去中心化金融系统的安全监管；
2. 研究区块链去中心化金融系统防护技术，面向针对去中心化金融体系的攻击行为和潜在资产风险，构建体系化的防护机制，通过交易拆分、拦截实现去中心化金融系统的高效防护；
3. 研究加密货币的历史交易跟踪和关联技术，可持续地输出面向比特币等2类加密货币的交易和交易方情报。

**研究输出成果：**

1. 区块链去中心化金融系统异常行为监测原型系统，并提供源代码；
2. 相关研究报告、高水平学术论文、发明专利等。

**2.漏洞挖掘与攻防对抗方向**

### 自动化智能化漏洞挖掘技术研究

随着软件规模和复杂度的日益增加，软件漏洞挖掘技术正逐渐向高度自动化和智能化演变。大规模的Fuzzing经常会产出海量的崩溃记录。崩溃记录是否来自一个新的漏洞？这个漏洞是否可以利用？应该如何利用这个漏洞？近年来采用机器学习技术缓解包括Fuzzing的漏洞挖掘领域的一些瓶颈问题，通过采用现有的机器学习、深度学习等技术，帮助相应的漏洞挖掘工具、系统在海量的漏洞相关的数据中提取经验和知识，然后根据训练生成的模型对新的样本进行分类、预测，提高对软件漏洞挖掘的精度和效率。

**研究方向包括但不限于：**

1. 研究自动化的漏洞本因分析、可利用性判定和利用工具生成技术，提供漏洞本质原因分析、可利用性判定和利用工具生成等功能的自动化漏洞分析的创新算法和工具；
2. 研究基于机器学习的漏洞挖掘算法，可应用二进制程序函数识别、函数相似性检测、脆弱路径筛选、高结构化输入生成、路径约束求解、测试输入筛选等多个不同场景；
3. 研究基于机器学习的代码词法、语法、控制流和数据流等静态特征进行分析和学习技术,发现真实的代码漏洞；
4. 研究构建通用漏洞检测模型或针对如缓冲区溢出、内存破坏等特定类型的漏洞进行分析及特征选取并进行模型构建。

**研究输出成果：**

1. 原型系统设计及算法，并提供源代码；
2. 相关研究报告、高水平学术论文、发明专利等。

### 供应链漏洞相关技术研究

2020年底的SolarWinds事件，使供应链安全再次成为热点，也印证了供应链安全是一个重要且复杂的课题，需要有一整套相应的理论、技术和方法，来管理、防护、处置相关漏洞。

**研究方向包括但不限于：**

1. 供应链漏洞管理技术研究；
2. 供应链漏洞防护技术研究；
3. 软件同源性分析技术研究。

**研究输出成果：**

1. 相关原型系统，并提供源代码；
2. 相关研究报告、高水平学术论文、发明专利等。

### 对抗攻击检测和防御体系技术研究

近几年来，深度学习技术经历了极大的发展，其性能在多个场景中已经超越人类的判断能力（如图像识别、语音识别等）。然而以Ian GoodFellow为首的深度学习学者们发现，深度学习系统可以被人类无法察觉的微小改动欺骗，在熊猫照片加入一个微小噪声后，深度学习系统会将熊猫误认成长臂猿。此类通过微小改动欺骗深度学习模型的方法被称为对抗攻击。对抗攻击给深度学习系统的大规模应用带来了极大隐患。例如，若自动驾驶的汽车误认交通牌则会造成交通安全隐患，若社交应用无法识别暴力恐怖信息则有可能危害社会治安。因此，针对对抗攻击的研究迫在眉睫。

**研究方向包括但不限于：**

1. 从攻击、防御、评估三方面研究对抗攻击的相关技术，如对抗攻击机理分析、对抗攻击样本生成技术、恶意样本探测技术、智能算法加固技术等；
2. 研制集成多种攻击与防御算法的原型系统，支持智能算法的高质量攻击、有效防御、系统评估等应用需求。

**研究输出成果：**

1. 相关原型系统，并提供源代码；
2. 相关研究报告、高水平学术论文、发明专利等。
   1. **自动化渗透测试技术研究**

渗透测试在发现网络脆弱性与评估网络安全状态方面发挥着重要作用，但是依赖安全专家花费大量时间和人力进行的方式已经不能满足高速增长的业务需要。当前虽然渗透测试工具不断涌现，但是目前渗透测试工具存在使用范围与场景碎片化、自动化程度低以及功能扩展难等问题；即便在特定场景通过预先配置能组合多种渗透测试工具，仍存在着如何快速、有效地进行攻击路径规划的问题。研究自动化渗透测试技术，对发现网络中存在的安全隐患、提升系统安全性，有十分重要的现实意义。

**研究方向包括但不限于：**

1. 研究自动化信息收集的技术，包括自动化收集信息技术和快速判断、筛选高价值信息的方法；
2. 研究智能化攻击路径规划技术，包括提高攻击面覆盖度、高危害攻击路径发现速度的方法。

**研究成果包括：**

1. 相关原型系统（一套自动化渗透测试原型系统，可验证快速、高效地自动化信息收集方法和攻击路径规划方法），并提供源代码；
2. 相关研究报告、高水平学术论文、发明专利等。
   1. **反欺诈技术研究**

近年来，网络黑产利用身份冒用及互联网应用、网络安全配置、系统等方面的漏洞,在线上融资、支付等环节进行欺诈的案件层出不穷。目前欺诈行业越来越呈现出产业化、隐蔽化、专业化、场景化的特征,对社会危害也越来越严重。研究欺诈产业新型技术手段、反欺诈的检查及应对能力是本课题的研究对象。

**研究方向包括但不限于：**

1. 涉诈URL识别场景，使用但不限于规则、机器学习等技术手段，实时对用户访问的URL进行检测，判定该URL是否涉诈；
2. GOIP诈骗电话识别场景，使用不限于话单等多源数据，检测手机卡或物联网卡是否用于GOIP电话诈骗；
3. 涉诈APP识别场景，采用静态分析、动态分析、内容安全监测、仿真等技术手段，识别给定的APP是否涉嫌诈骗，同时输出该APP的诈骗类型。

**研究成果包括：**

1. 相关原型系统，并提供源代码；
2. 相关研究报告、高水平学术论文、发明专利等。
   1. **移动应用攻击面自动检测技术研究**

随着智能手机和iPad等移动终端设备的普及，人们逐渐习惯了使用应用客户端上网的方式，而智能终端的普及不仅推动了移动互联网的发展，也带来了移动应用的爆炸式增长。在网络攻防对抗中，随着移动应用的越来越普及，一些能够为商业红队所利用的攻击入口也相继暴漏。同时相比于一般互联网的资产，由于其检测门槛较高，自动化批量检测工具缺乏，开发周期较短等问题，其更容易产生可利用的攻击面。如何能够发现这些交互接口并形成自动化发现流程，针对移动应用架构、客户端及后端存在的威胁等多方面进行威胁面分析检测，发现其中的薄弱环节，为商业红队提供快速的攻击面，是本项目关注的重点。

**研究方向包括但不限于：**

1. 研究[ANDROID](https://www.cnblogs.com/qswz/p/12783012.html)环境下的小程序、微信公众号、APP等移动应用的网络攻击面自动化检测方法；
2. 研究IOS环境下的小程序、微信公众号、APP等移动应用的网络攻击面自动化检测方法。

**研究输出成果：**

1. 相关原型系统（包含移动应用攻击面自动化检测）；
2. 相关研究报告、高水平学术论文、发明专利等。

# 3.云计算安全与网络空间安全方向

### 多云混合云的安全能力编排技术研究

多云与混合云将是未来企业上云的必然趋势，复杂的IT环境增加了安全防护的难度，例如各种形态的安全产品资源管理，网络流量的调度和安全策略的编排将会变得非常复杂，此外，攻击者可能会通过公有云攻陷资产渗透进企业内网，因而多云与混合云的全面一致的安全防护的要求会非常现实，而如何统一管理、调度和编排安全资源和能力将是未来需要解决的首要科学问题。

**研究方向包括但不限于：**

1. 研究多云与混合云场景下的安全资源、安全策略自动化编排技术，设计统一的安全策略模型和编排体系，设计面向多云和混合云的访问控制、资源隔离等不少于5类安全策略，支持不少于10类安全SaaS和虚拟化、容器化的安全设备；
2. 研究安全策略冲突发现和缓解技术。

**考核指标：**

1. 相关原型系统，并提供源代码；
2. 相关研究报告、高水平学术论文、发明专利等。

### 零信任网络中基于向量表征与计算的访问控制技术研究

传统访问控制模型中，访问主体通过角色属性获取相应权限。但是在零信任架构下，以前的相对静态的或者相对封闭的网络环境已经越来越少，逐步向开放式发展，访问主体身份不固定，频繁进行登录和退出操作，对于访问控制模型提出了更高要求：在零信任环境下，为保证系统的安全性，需要时刻对用户的访问行为进行实时访问控制，这为传统的基于规则匹配的访问控制模型带来了极大的计算压力。

通常的访问控制规则匹配，都需要计算机进行基于模式匹配的计算；在零信任环境下，每时每刻进行基于规则匹配的访问控制极其低效。此外，访问控制是网络空间安全的基础支撑技术，当前的基于形式化语言描述的访问控制技术，在零信任环境下或云资源访问控制环境下会面临“规则爆炸”、“组合爆炸”的瓶颈。

在已有的访问控制规则库、数据集中，蕴含了大量的访问控制知识信息。如果能够通过某种方式，赋予计算机“理解、运用”这些安全知识的能力，使计算机以其所擅长的“数值计算”的方式，以极低的运算复杂度实时“计算”出访问控制的判定结果，则会大大提高零信任环境下访问控制匹配的效率。

**研究方向包括但不限于：**

1. 研究在大数据和零信任环境中运用AI技术或其他技术解决安全访问控制规则爆炸情况下的访问速度问题；
2. 研究访问控制规则中规则互斥问题；
3. 研究可计算性访问控制行为模式识别与推理技术，实现零信任网络环境下开放的、智能的访问控制。

**研究输出成果：**

1. 相关原型系统（包含零信任网络环境下的快速访问控制模型），并提供源代码；
2. 相关研究报告、高水平学术论文、发明专利等。

### 企业攻击暴露面测绘技术研究

传统的网络资产测绘技术主要采用主动性的网络探测和被动流量分析为主。在公网地址资产测绘方面，主动性网络探测使用较多。在企业网络边界的流量设备上基于流量的特征分析方式较为常见。随着攻防博弈的交替升级，黑客也在研究和使用包括信息收集在内的多种测绘手段结合等方式，完成目标资产的测绘和脆弱点收集；此外，攻击者关心的资产从传统的IT主机和服务，扩展到了整条攻击路径中的各类资产、网络、供应链和人员等实体。

从而，应对此类攻击暴露面（Attack Exposure Surface）测绘，防守方应当未雨绸缪，从宏观监测和风险评估视角，模拟真实的黑客攻击思路，研究一种新型智能的测绘技术，结合传统方式，对企业内部各类广义资产进行测绘和风险评估是本课题研究的目标。

**研究方向包括但不限于：**

1. 研究企业内外部广义资产和实体的发现和识别技术，包括但不限于各类IT资产、供应链、网络拓扑、边界安全设备等；
2. 研究基于知识图谱的各类广义资产和实体的关系测绘技术；
3. 研究企业网络脆弱点识别和网络突破技术，研究智能化的攻击与攻陷模拟技术；
4. 研究智能化的企业人员组织、安全意识测绘技术。

**研究输出成果：**

1. 相关原型系统，并提供源代码；
2. 相关研究报告、高水平学术论文、发明专利等。

### 数字经济中新型基础设施的安全风险评估技术研究

在数字经济时代，涌现出的新型技术正在驱动新一轮科技革命和产业变革，成为数字经济发展的基石。以5G、车联网、区块链等为代表的新型基础设施，正在成为支撑经济社会数字化发展的基础设施体系，将关系着国计民生，是未来经济社会运行的神经中枢，网络空间安全的重中之重。当前网络空间军事化、网络武器平民化、网络攻击常态化的态势日趋明显，这些新型基础设施未来极可能成为网络攻击的主要目标。相比常见的勒索病毒、数据泄露等常见的攻击手段，针对这些特定行业的新型网络攻击面研究，具有行业特性的研究是本课题需要关注的重点。

此外，国家关键信息基础设施是指关系国家安全、国家公共利益的信息设施，包括但不限于提供公共通信、广播电视传输等服务的基础信息网络、能源、金融、交通、水利等领域的关键系统等。关键基础设施关系着国计民生，是经济社会运行的神经中枢，是网络安全的重中之重。随着经济社会对网络的依赖程度不断加深，关键信息基础设施安全防护更加紧迫。网络空间军事化、网络武器平民化、网络攻击常态化的态势日趋明显，关键信息基础设施越来越成为网络攻击的主要目标。相比常见的勒索病毒、数据泄露等常见的攻击手段，针对特定行业的新型网络攻击面研究，具有行业特性的研究是本课题需要关注的重点。

**研究方向包括但不限于：**

1. 面向5G、车联网、工业互联网、数字/加密货币、天地一体化等安全风险评估方法的研究，研究相关攻击对特定行业、整体社会造成的危害及损失评估方法；
2. 研究5G核心网与无线网相关攻防技术；
3. 研究区块链智能合约安全技术，研究面向加密货币的黑灰产团伙跟踪；
4. 研究我国航空、高铁和地铁等交通行业中关键核心业务系统的攻击面；
5. 研究面向电网的高功率物联网设备僵尸网络的攻防及影响范围。

**研究输出成果：**

1. 结合真实业务场景形成典型攻击场景分析样例；
2. 新型基础设施的脆弱性分析方法和攻击面梳理，及相关的危害影响评估模型；
3. 相关原型系统，并提供源代码；
4. 相关研究报告、高水平学术论文、发明专利等。

# 4.工业物联网安全与协议安全方向

### 面向工业物联网的威胁评判和处置方法研究

随着工业物联网技术的发展，技术的革新在给公司带来创收的同时，也引入了相关的安全风险。物联网的多源异构性、开放性、泛在性使公司的业务安全性面临潜在的巨大威胁。相比于PC互联网和移动互联网，公司物联网覆盖领域广泛，接入设备数量大，应用地域和设备供应商标准分散，物联网的应用多样性和复杂性远超互联网。相对于传统IT安全，物联网安全具有攻击面大、数据量大的特点，需要对海量物联网终端、网络流量、业务平台、安全系统和安全设备等数据进行处理。通过海量数据分析，发现未知威胁、预测潜在风险和自适应联动响应安全事件。

**研究方向包括但不限于：**

1. 研究基于工业业务属性的动态感知技术和安全管控技术；
2. 研究物联网和边缘计算场景下网络安全事件监测机制，研制适配专用探针的物联网场景下网络安全事件监测、恶意样本检测引擎，适配Snort、MTX等语法描述，提供物联网相关网络威胁识别网络风险明文规则3.5万条，提交上述知识库的明文特征规则；
3. 研究多数据业务融合的安全智能处置和业务自适应处置和编排技术；
4. 研究基于边界、主机和控制内建安全策略的策略优化机制。

**研究输出成果：**

1. 相关原型系统，并提供源代码；
2. 相关研究报告、高水平学术论文、发明专利等。

### 工业协议识别技术的研究及应用

工业领域由于涉及多种应用行业和场景对于操作的内容、实时性要求存在一定的差异性，导致不同的应用在协议定义上存在很大的差异。工业协议在工业通信中承担在数据采集和操作控制的功能，其在工业整个运行中所占有比较重要的地位。同时由于工业协议众多，各个协议之间又存在这交大的差异性。原有对于协议的识别通过数据抓取和分析的方式存在无法穷举所有协议重要操作字段的问题，存在需要大量人工接入分析和处理效率普遍比较低的问题，存在无法准确感知数据内容的问题。

**研究方向包括但不限于：**

1. 研究面向未知工业协议的自动化识别算法模型，提供工业协议上下文分析的关联分析算法，可以在火电、精细化工、汽车制造业行业验证；
2. 研究操作协议关键操作和关键字段的之间的内在联系，研究不少于20种的协议的深度分析模型，可以分析出关键操作指令和关键值域的操作范围等；
3. 研究工业控制协议深度解析技术，研制一套高效自适应的工控协议深度解析方案，至少识别FOCAS协议、三菱机床的数控协议、FOXCON协议、艾默生OVATION DCS协议，恒河电机工业协议等不少于20个厂家的60种工业协议

**研究输出成果：**

1. 相关原型系统，及提供可验证的未知协议分析的算法模型源码；
2. 相关研究报告、高水平学术论文、发明专利等。

### 智能传感网安全技术研究

伴随着工业互联网的发展，对于数据的采集和分析提出了更高的要求，智能化的传感器对于不同数据的感知能力，一次性的处置能力，微小化的易部署特性，已经成为工业互联网领域的真正神经末梢，支撑起工业互联网基础运行部件的状态感知、数据的基础分析。尤其是MEMS传感器继承了集成电路的先进制造工艺，具有微型化、智能化、集成化、成本低、效能高等优势，非常适合于工业互联网领域中基础运行部件的智能化改造以及相关的数据采集和分析。在大量传感器的应用下，网络安全风险在进一步的加剧，对于传感器数据的篡改，修改传感器的参数，DOS传感知使传感器失去可用性等问题，潜在可能被勒索病毒攻击导致文件被加密无法使用。

**研究方面包括但不限于：**

1. 研究基于传感网运行机理的威胁模型；
2. 研究传感器嵌入式系统的脆弱性；
3. 研究融合物理安全、功能安全与网络安全的融合的异常感知算法；
4. 研制安全防护和感知能力集成化的基础智能传感器部件；
5. 研制智能传感网形成一体化解决方案。

**研究输出成果：**

1. 相关智能传感网安全风险研究报告；
2. 相关集成安全功能的智能传感器；
3. 相关异常模型算法原型系统，并提供源代码；
4. 相关高水平学术论文、发明专利等。